Bloque IV: El nivel de red

Tema 10: Subredes

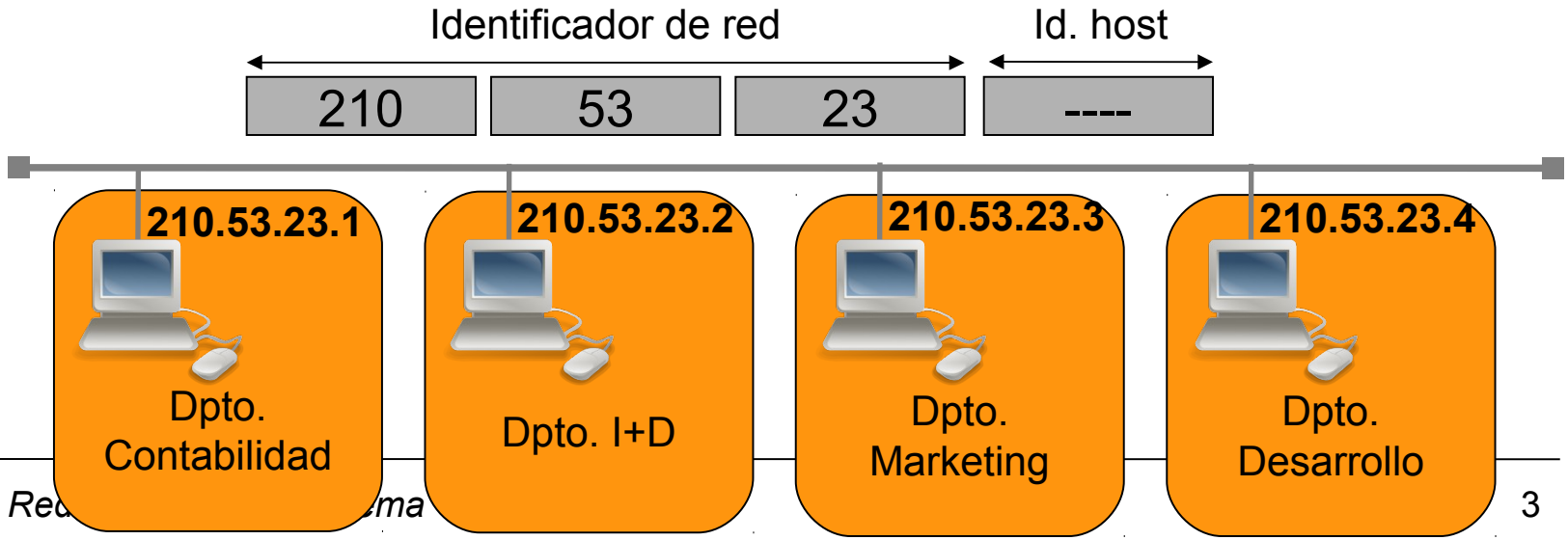
Índice

- Bloque IV: El nivel de red
  - Tema 10: Subredes
    - Introducción
    - Máscara de subred
    - Direcciones de subred
    - Subredes de tamaño variable
    - DHCP
    - NAT

- **Lecturas recomendadas:**
  - Capítulo 4, sección 4.4.2, de “Redes de Computadores: Un enfoque descendente”. James F. Kurose, Keith W. Ross. Addison Wesley.

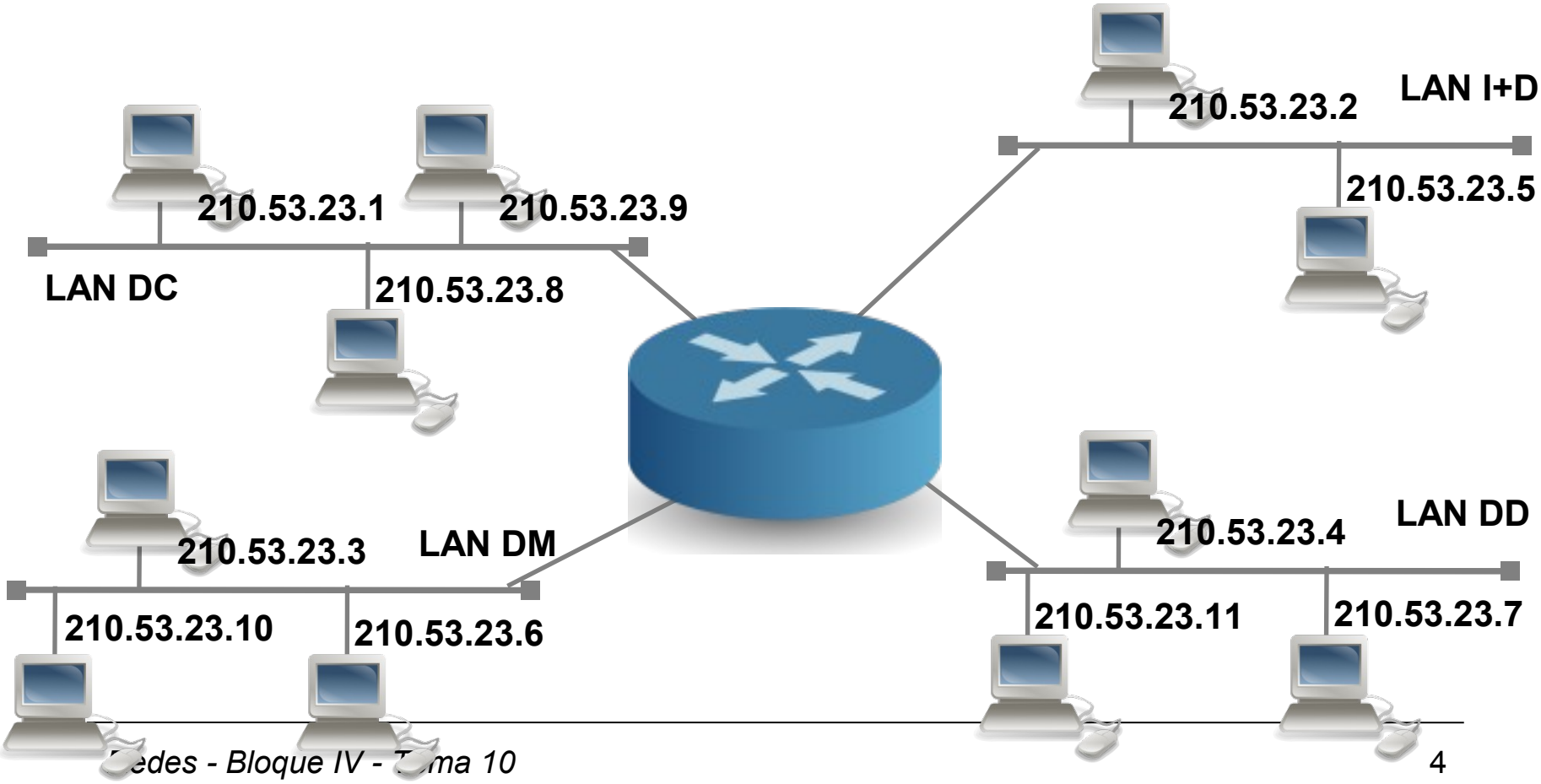
Introducción

- Subredes: consiste en dividir una red en partes mas pequeñas.
  - Nivel jerárquico intermedio entre red y host.
  - Utiliza unos bits de la parte del identificador de host para la subred.
  - Organización jerárquica de la red→ Visión externa como una sola red, aunque dividida en subredes.
- Por ejemplo, partimos de una dirección clase C: 210.53.23.0
  - Tenemos una empresa y 4 departamentos.
  - Inicialmente no realizamos ningún tipo de división, porque la empresa es demasiado pequeña.



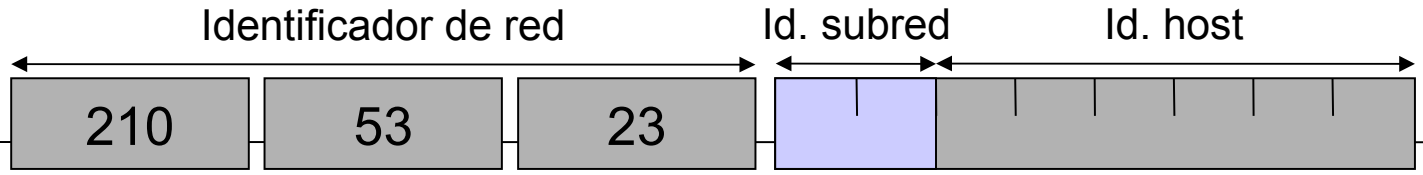
Introducción

- Pero la empresa crece, y cada departamento necesita una LAN → Solución: asignar aleatoriamente las direcciones IP.
- Problema: la tabla de enrutamiento para el router es enorme (necesito una entrada para cada máquina).



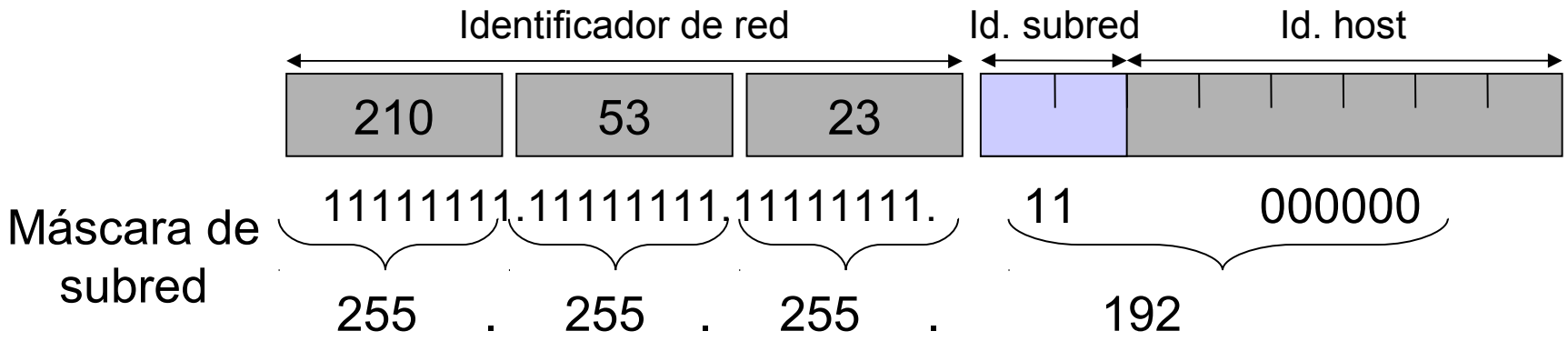
Introducción

- Solución → Subredes: dividir el espacio de direcciones en 4 grupos.
  - 0-255
    - 0-63 para el dpto. de contabilidad
    - 64-127 para el dpto. de I+D
    - 128-191 para el dpto. de marketing
    - 192-255 para el dpto. de desarrollo
- Y en binario:
  - 0-255
    - 0-63 = 00 XX XXXX
    - 64-127 = 01 XX XXXX
    - 128-191 = 10 XX XXXX
    - 192-255 = 11 XX XXXX
- **Identificador de subred**: con los 2 primeros bits del identificador de host, sabremos a que departamento (subred) pertenece una máquina.



Máscara de subred

- Indica cuantos bits forman el identificador de red y subred, y cuantos forman el identificador host.
  - Se ponen a 1 todos los bits correspondientes al identificador de red o subred.
  - Se ponen a 0 todos los bits correspondientes al identificador de host
- Cada máquina almacena su dirección IP y su máscara de subred.



- Una dirección IP siempre tiene una máscara asociada: 210.53.23.65 y 255.255.255.192
- Otra notación más breve: 210.53.23.65**/26** (se utilizan 26 bits para identificador de red y subred).

Máscara de subred: Ejercicio

- Indica los bits de identificador de red, subred y host para las siguientes IPs y máscaras:

10.58.26.129 255.255.0.0	181.23.117.89 255.255.255.0	198.58.201.89 255.255.255.0
bits red: bits subred: bits host:	bits red: bits subred: bits host:	bits red: bits subred: bits host:
10.58.26.129 255.255.240.0	181.23.117.89 255.255.254.0	198.58.201.89 255.255.255.192
bits red: bits subred: bits host:	bits red: bits subred: bits host:	bits red: bits subred: bits host:

Direcciones de subred

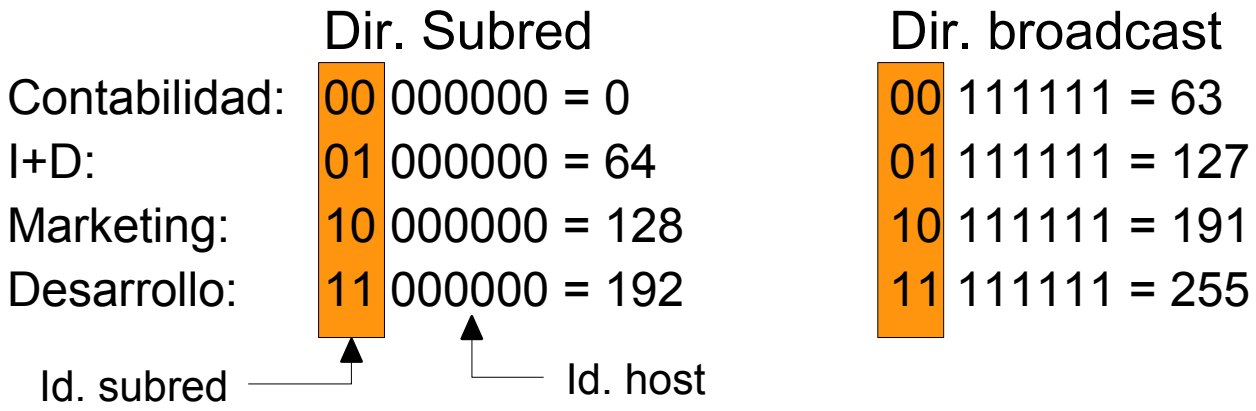
- Direcciones IP reservadas: en cada subred hay dos direcciones reservadas → la dirección de subred y la de broadcast en la subred.

- **Dirección de subred**:
  - Dirección IP que identifica a una subred.
  - Se calcula para cada subred poniendo a 0 el identificador de host.
  - Coincide con la primera IP del rango.
  - Es equivalente a: dirección IP AND máscara de subred.

- **Dirección de broadcast en la subred**:
  - Se calcula poniendo todo a 1 el identificador de host.
  - Coincide con la última IP del rango.
  - Representa a todas las máquinas de la subred.Nº

Direcciones de subred

- Calcular las direcciones de subred y de broadcast del ejemplo:



Subred	Rango	Máscara	Dir. subred	Dir. broadcast
Contabilidad	210.53.23.0-63	255.255.255.192	210.53.23.0	210.53.23.63
I+D	210.53.23.64-127	255.255.255.192	210.53.23.64	210.53.23.127
Marketing	210.53.23.128-191	255.255.255.192	210.53.23.128	210.53.23.191
Desarrollo	210.53.23.192-255	255.255.255.192	210.53.23.192	210.53.23.255

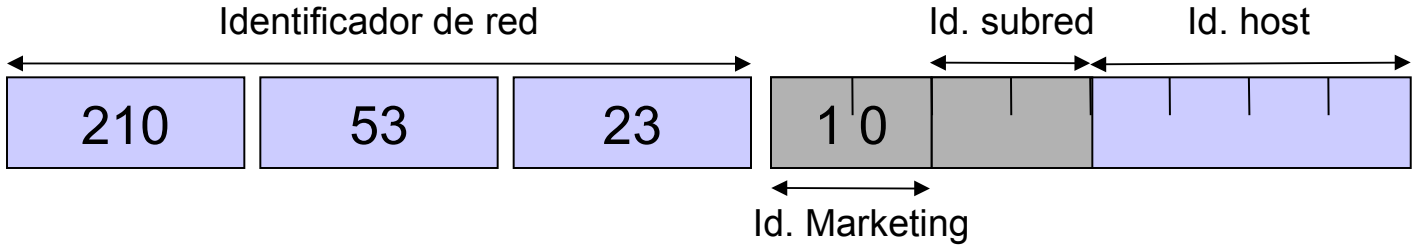
Direcciones de subred

- Nº subredes = $2^{\text{bits subred}}$ Nº hosts = $2^{\text{bits host}} - 2$
- Subredes y hosts para una red clase C:

Bits subred	Nº subredes	Bits host	Nº hosts	Máscara	Máscara binario
0	0	8	254	255.255.255.0	0000 0000
1	2	7	126	255.255.255.128	1000 0000
2	4	6	62	255.255.255.192	1100 0000
3	8	5	30	255.255.255.224	1110 0000
4	16	4	14	255.255.255.240	1111 0000
5	32	3	6	255.255.255.248	1111 1000
6	64	2	2	255.255.255.252	1111 1100
7	128	1	0	255.255.255.254	1111 1110
8	256	0	0	255.255.255.255	1111 1111

Subredes de tamaño variable

- Subredes de tamaño variable o sub-subredes:
  - El departamento de marketing (subred 210.53.23.128) se quiere subdividir en 4 subredes.



Subred	Rango	Máscara	Dir. subred	Dir. subred
Marketing 1	210.53.23.128-143	255.255.255.240	10 00 0000	210.53.23.128
Marketing 2	210.53.23.144-159	255.255.255.240	10 01 0000	210.53.23.144
Marketing 3	210.53.23.160-175	255.255.255.240	10 10 0000	210.53.23.160
Marketing 4	210.53.23.176-191	255.255.255.240	10 11 0000	210.53.23.176

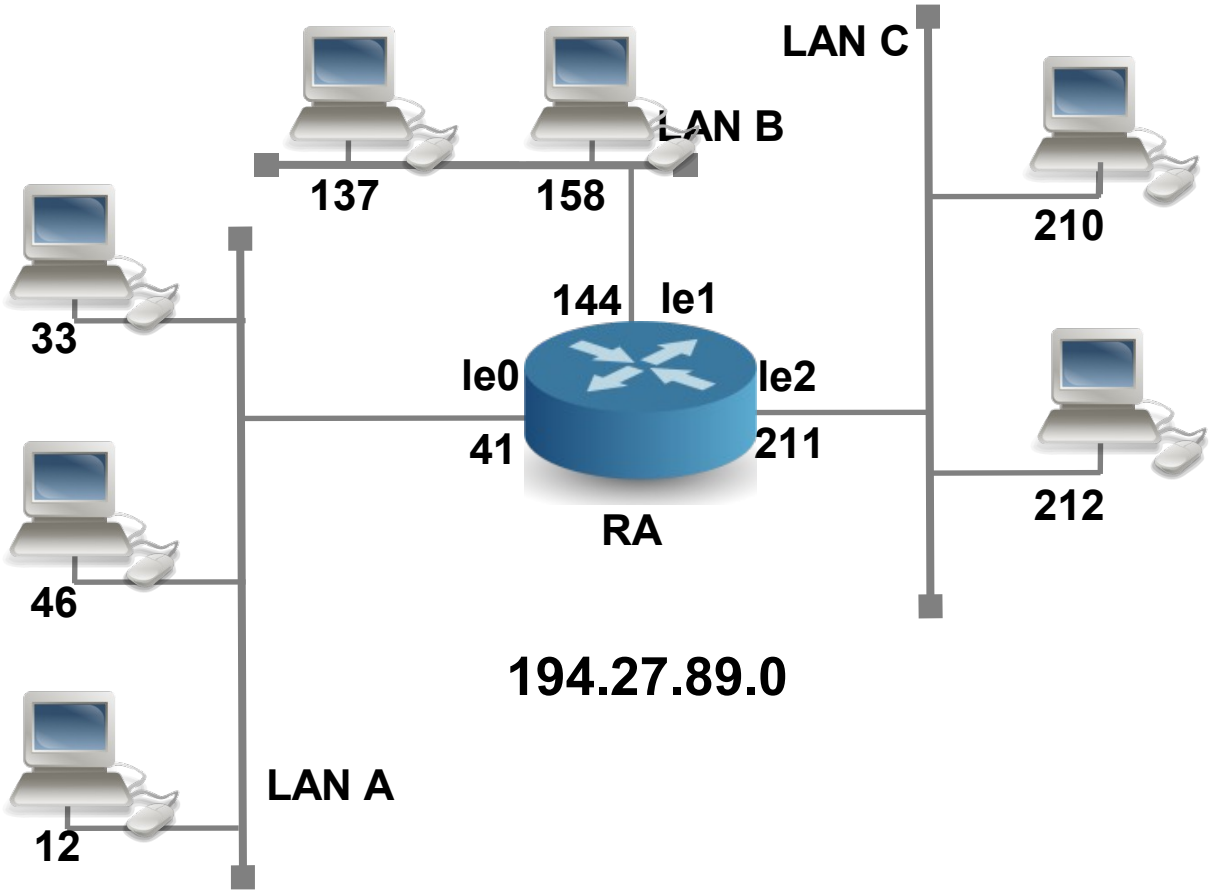
Subredes: Ejercicio 1

- Queremos organizar la red de nuestra empresa, teniendo en cuenta la siguiente distribución por departamentos:
  - Dpto. contabilidad: 12 ordenadores
  - Dpto. I+D: 18 ordenadores
  - Dpto. desarrollo: 21 ordenadores
    - Análisis: 8 ordenadores
    - Implementación: 13 ordenadores
  - Dpto. marketing: 10 ordenadores
  - Dpto. administración: 10 ordenadores
- Disponemos de una dirección clase C: **195.35.12.0**

- Calcular la máscara de subred, id de red y rango de IPs de cada subred.

Subredes: Ejercicio 2

- Calcular las máscaras de subred, id subred y dirección de broadcast de subred, de A, B y C



Subredes: Ejercicio 2

- 33 = 0010 0001
- 46 = 0010 1110
- 12 = 0000 1100
- 41 = 0010 1001

Subred	Máscara (bin)	Máscara
A		
B		
C		

- 137 = 1000 1001
- 158 = 1001 1110
- 144 = 1001 0000

Subred	Id. subred (bin)	Id. subred
A		
B		
C		

- 210 = 1101 0010
- 211 = 1101 0011
- 212 = 1101 0100

Subred	Broadcast (bin)	Broadcast
A		
B		
C		

DHCP: Funcionamiento

- Modelo cliente-servidor basado en UDP: puerto 67 para el servidor y 68 para el cliente.
- Mensajes DHCP: el cliente incluye un identificador de transacción en el mensaje de descubrimiento, que deberá ser repetido en los siguientes.
  - **Discovery**: mensaje difundido en la red por el cliente para descubrir el/los servidores DHCP.
  - **Offer**: mensaje que contiene la dirección IP que el servidor ofrece al cliente DHCP.
    - Incluye la dirección MAC del cliente, la IP ofertada, la máscara, el tiempo de validez y la dirección del servidor.
  - **Request**: el cliente seleccionará una dirección de las ofertadas.
    - En caso de existir varios servidores, se indica el servidor del que se acepta la oferta.
  - **Acknowledgement**: el servidor confirma la solicitud del cliente y le indica cualquier otra información solicitada por el cliente.
- El cliente no tiene dirección IP → Todos los mensajes tienen como destino la dirección de **broadcast** 255.255.255.255

DHCP

- Una vez que la red está organizada ⇒ Asignar direcciones IP.
  - Normalmente, a los routers se les asigna manualmente.
  - ¿Y a los hosts …?
- Dynamic Host Configuration Protocol: permite asignar direcciones IP dinámica y automáticamente a los hosts (**plug-and-play**):
  - Las direcciones IP se asignan durante un tiempo limitado (desde horas a días), después es necesario renovarlas.
  - También incluye otros parámetros como máscaras de subred, router por defecto (antes se utilizaba ICMP o BOOTP) y servidores DNS.
- Se basa en el modelo cliente-servidor
  - Cliente DHCP: cualquier máquina "nueva" en la red que se esté iniciando y necesite una configuración de red
  - Servidor DHCP: garantiza que todas las direcciones IP son únicas (durante su tiempo de vida).
- Métodos de asignación de direcciones:
  - Estática o manual: se asigna una dirección IP a una máquina concreta (en base a su dirección MAC). Evita que se conecten clientes no identificados.
  - **Dinámica**: se utiliza un rango de direcciones IP y cada ordenador de la red está configurada para solicitar su dirección IP al iniciarse la interfaz.
    - Permite la reutilización dinámica de las direcciones IP.
    - Facilita la instalación de nuevas máquinas en la red.
  - Automática: similar al modo Dinámico, pero un equipo siempre obtiene la misma IP.

DHCP: Alternativa

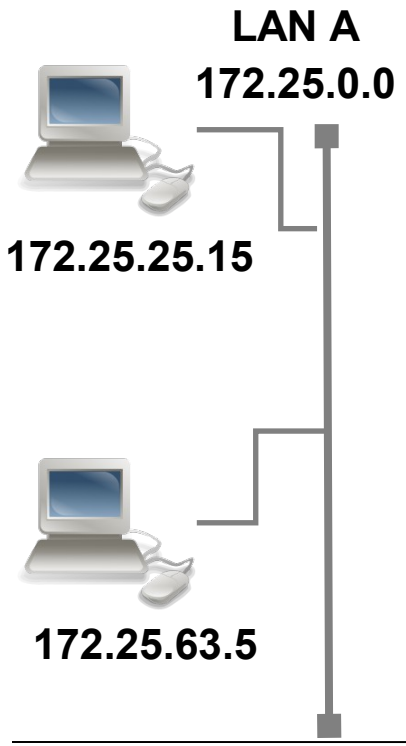
- ¿Y qué pasa si no hay un servidor DHCP en mi red?
- Se definen las direcciones IP **link-local**: **169.254.0.0/16**
- APIPA (Automatic Private IP Addressing): permiten a un host auto-asignarse una IP para poder operar en una LAN cuando no hay ningún tipo de servidor disponible:
  - Se escoge una IP del rango aleatoriamente.
  - Se comprueba mediante ARP que nadie la tiene asignada.
  - En cuanto obtiene una IP “válida”, deja de usarse.

NAT: Direcciones privadas

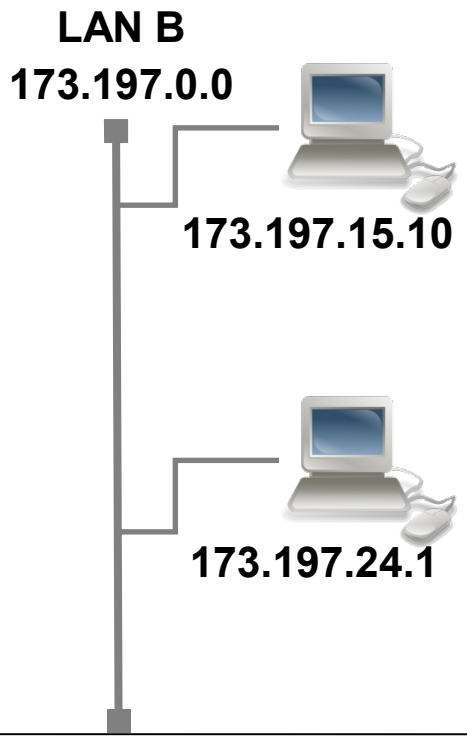
- Cuando contratamos una banda ancha, mi ISP me proporciona **una** dirección IP, pero ¿y si quiero conectar más de un dispositivo a Internet?
  - Varios PCs, consolas, teléfonos, TV, ...
- Direcciones IP públicas: identifican unívocamente un dispositivo en Internet.
- **Direcciones IP privadas**: exclusivamente para uso interno.
  - Los dispositivos de la red privada se pueden comunicar entre si con esas direcciones.
  - Pero no se pueden comunicar con el exterior (Internet) ⇒ Solución: NAT.
- Rangos de direcciones IP privadas:
  - Clase A: **10.0.0.0** (1 red)
  - Clase B: **172.16.0.0 – 172.31.0.0** (16 redes)
  - Clase C: **192.168.0.0 – 192.168.255.0** (256 redes)

NAT: Direcciones privadas

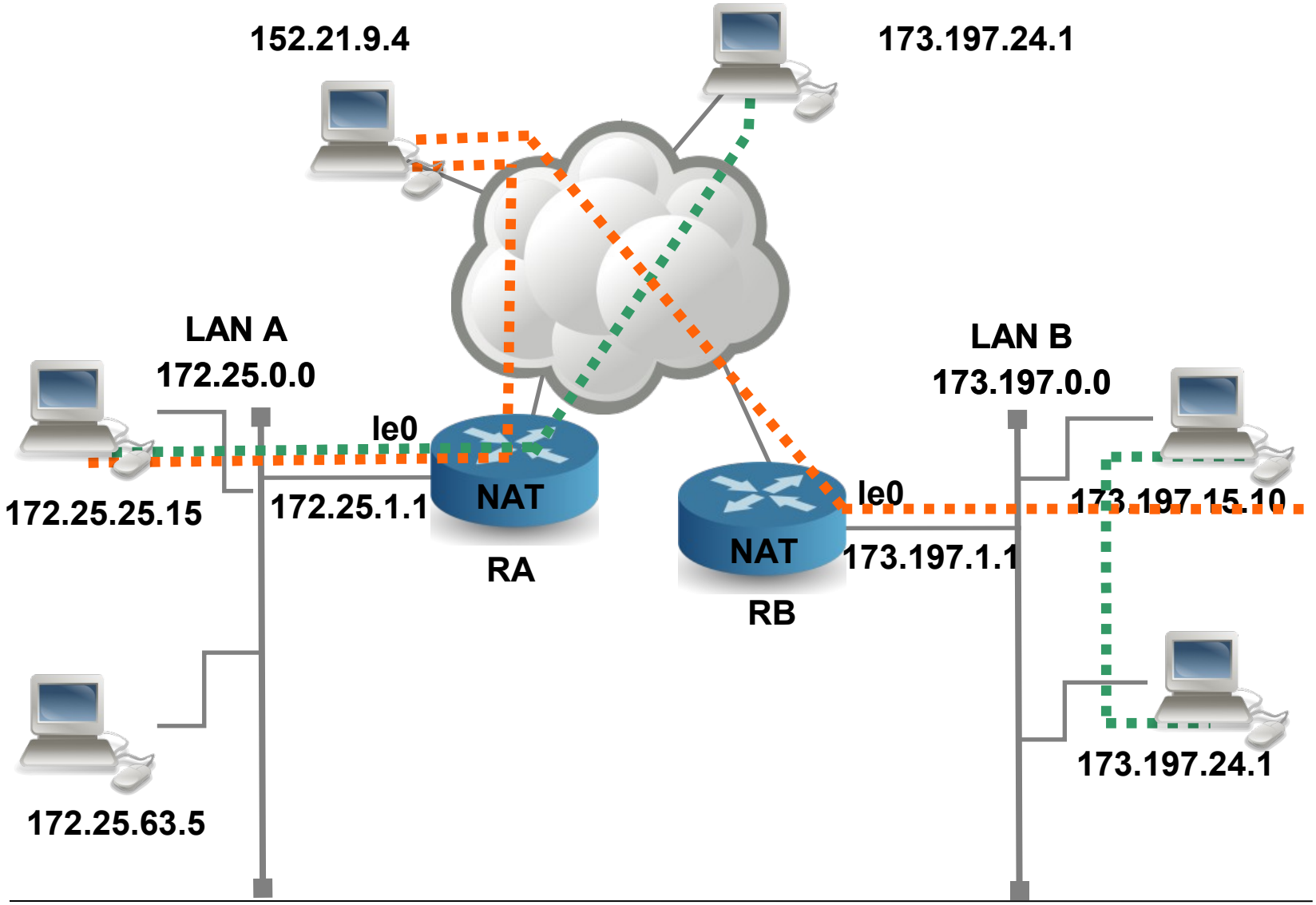
- Red doméstica A, utilizando una dirección privada.



- Red doméstica B, utilizando una dirección pública.



NAT: Direcciones privadas

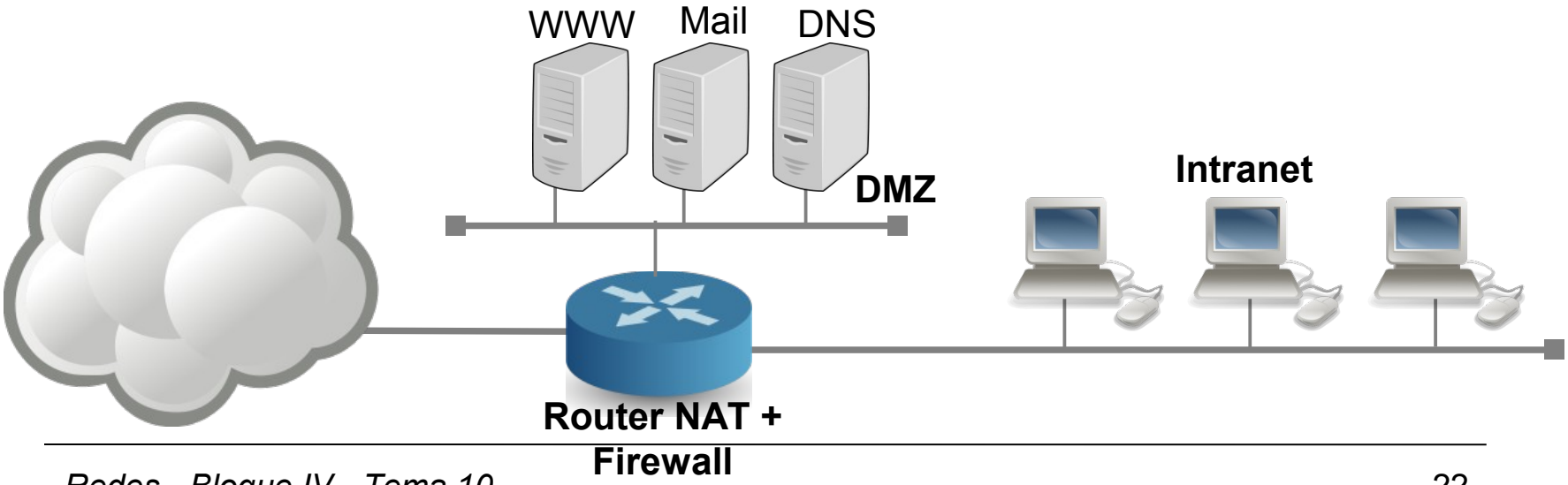


NAT

- **Network Address Translation**: consiste en modificar la dirección IP origen y/o destino de un datagrama IP al pasar a través de un router o firewall:
  - Permite a múltiples máquinas en una red privada acceder a Internet usando una única dirección IP pública.
- Surge debido a dos problemas: escasez de direcciones IP y escalabilidad del enrutamiento.
  - También ofrece seguridad: no se admiten conexiones desde fuera.
- Tipos de NAT:
  - **NAPT** (Network Address Port Translation): múltiples máquinas comparten una única dirección IP pública → La traducción se realiza mapeando números de puerto.
  - **Basic NAT** (o NAT estático o NAT 1 a 1): sólo se realiza el mapeo de direcciones IP → Cada dirección IP privada tiene asignada una dirección IP pública.

NAT

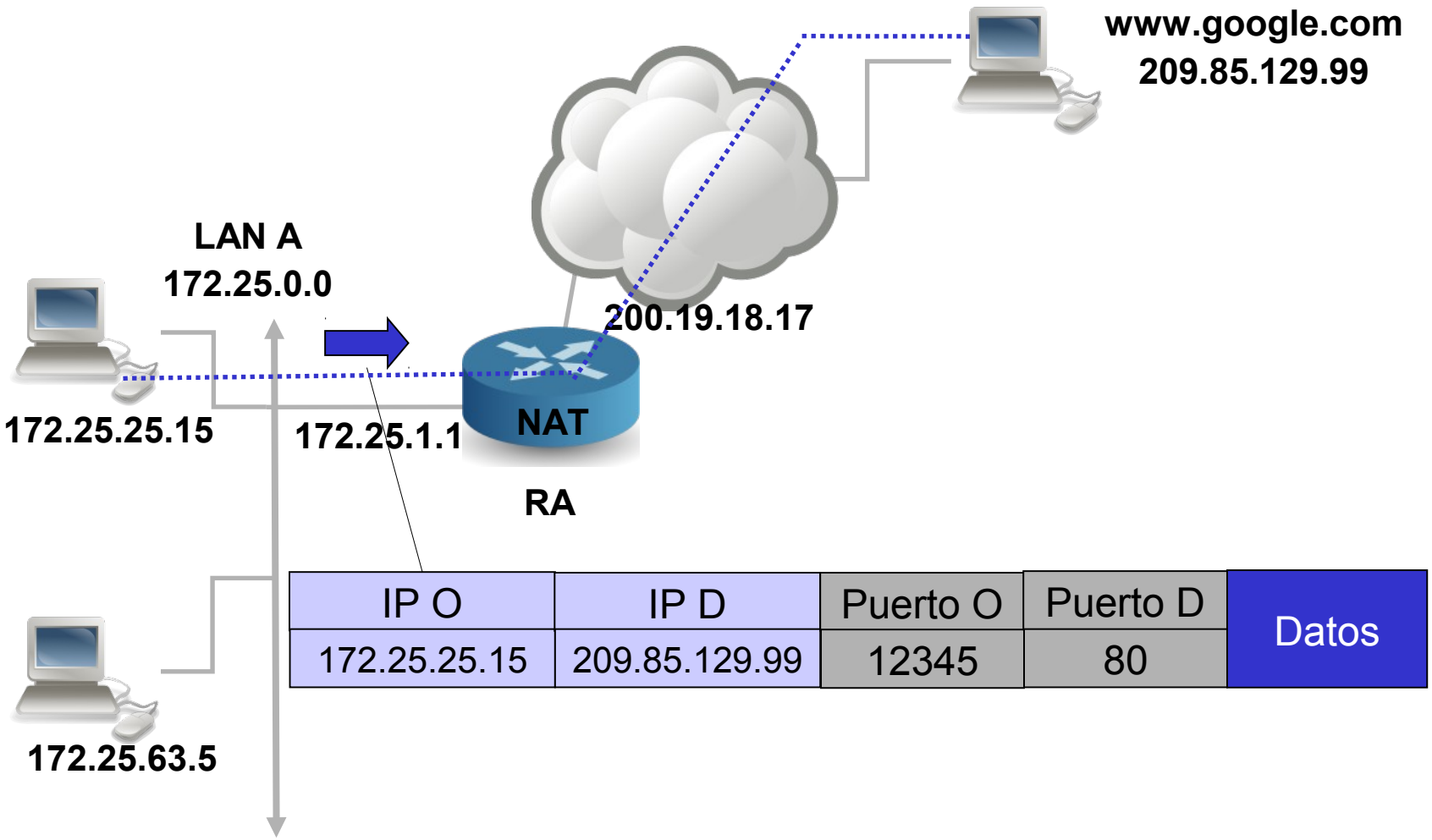
- Configuración típica:
  - La red interna (intranet) utiliza una dirección IP privada.
  - El router de la red tiene una interfaz con IP privada (conectada a la red interna) y otra interfaz con IP pública (conectada a Internet).
  - El router se encarga de realizar NAT e incluye un firewall.
  - Desde Internet parece que la comunicación se está realizando directamente con el router.
  - Los servidores públicos se incluyen en una red independiente (DMZ).



NAT

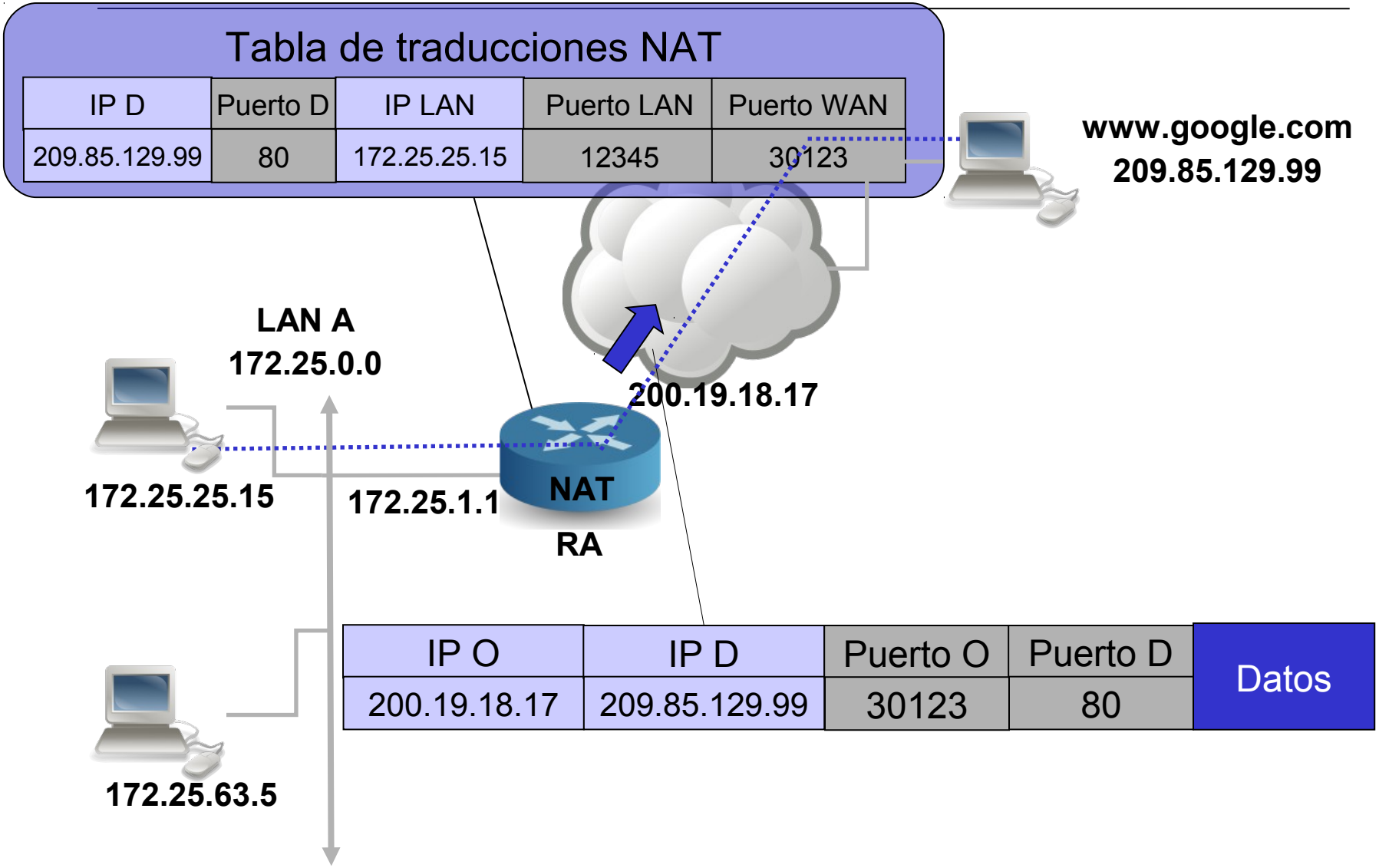
- **DMZ** (DeMilitarized Zone): parte de una red que se sitúa entre la red interna de una organización e Internet:
  - Se permiten las conexiones desde las redes externa e interna al DMZ.
  - Desde el DMZ sólo se permiten las conexiones a la red externa → Esto protege la red interna en caso de que una máquina de la DMZ sea comprometida.
  - En la DMZ se incluyen todos los servidores accesibles desde el exterior: servidor Web, correo electrónico, DNS, …
- **Firewall**: dispositivo configurado para permitir, denegar o actuar de intermediario en las comunicaciones de una red.
  - Puede ser hardware o software.
  - Permite controlar el tráfico entre redes de diferentes zonas de confianza.
  - Normalmente, separa una red interna (intranet: alto nivel de confianza) de una red externa (Internet: confianza nula), evitando accesos irregulares a la red interna.
  - Por ejemplo: *iptables*.

NAPT: Funcionamiento

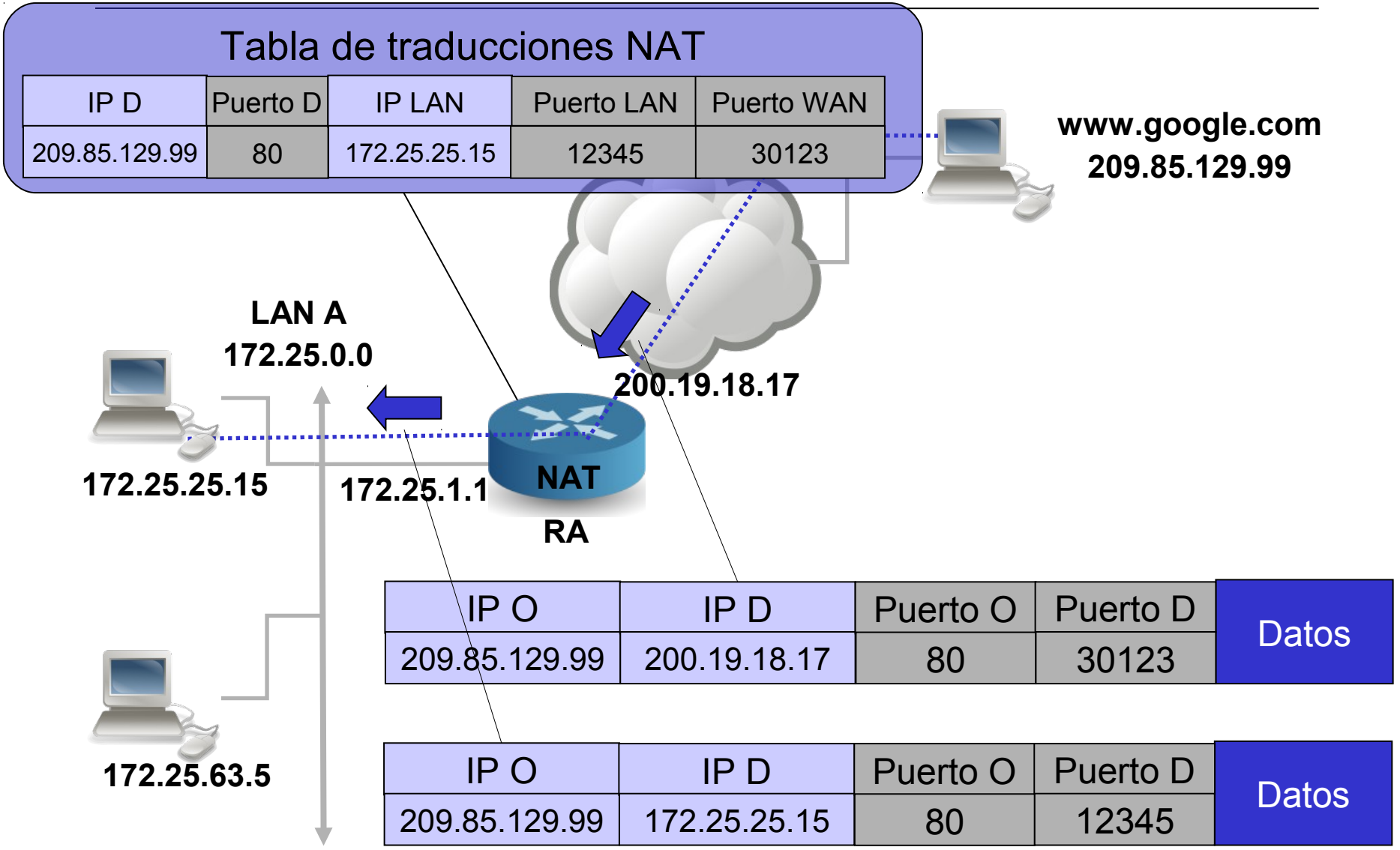


IP O	IP D	Puerto O	Puerto D	Datos
172.25.25.15	209.85.129.99	12345	80	

NAPT: Funcionamiento



NAPT: Funcionamiento



NAT

- Ventajas:
  - Seguridad: no se permiten conexiones bidireccionales: una máquina interna debe iniciar la conexión con una máquina de Internet → Evita conexiones maliciosas desde el exterior.
  - Solución para la escasez de direcciones IPv4:
    - Utilizar direcciones IP públicas sólo para máquinas que requieran conexión bidireccional a Internet.
    - Direcciones privadas para las máquinas que sólo se conectan a Internet.
- Inconvenientes:
  - No existe una conectividad extremo a extremo real:
    - Se usan los números de puerto para direccionar hosts, no procesos.
    - Los routers sólo deberían implementar hasta el nivel de red.
  - Es un parche para la escasez de direcciones, cuando IPv6 soluciona el problema de raíz.
  - **NAT Traversal**: plantea problemas en las aplicaciones que requieren que se inicien conexiones desde el exterior (p.e. FTP) → Desarrollo de técnicas específicas para estos casos (p.e. FTP pasivo).

NAT y UPnP

- Universal Plug and Play
- Solución para NAT Traversal:
  - Un host puede descubrir y configurar un router NAT de su red.
  - Permite a hosts externos iniciar comunicaciones TCP o UDP con hosts de una red privada a través de NAT.
- Funcionamiento:
  - Una aplicación de un host privado puede solicitar la correspondencia NAT entre su IP privada y puerto privado, con la IP pública (del router NAT) y un puerto público.
  - Si el router NAT acepta la solicitud, se crea la asociación → Se pueden conectar desde el exterior.
  - Además, la aplicación puede conocer la IP y el puerto público y anunciarlos.